Traffic Analysis – Decrypting HTTPS Malware Traffic

Date: August 1, 2025
Tool Used: Wireshark
Focus: Encrypted Traffic Analysis (HTTPS) | Malware Identification | Network Forensics

Analysed a packet capture (PCAP) from a Dridex malware infection on a Windows 10 machine. All web traffic was encrypted via HTTPS (TLS), and no session key or key log file was provided. The objective was to extract meaningful indicators and identify malicious behaviour without decrypting payloads.

Key Findings

Encrypted Communication:

Despite TLS encryption, valuable indicators were extracted from SNI fields, IP patterns, and request metadata.

Infected Device:

Identified as 10.4.1.101 (hostname: DESKTOP-U54AJ8K) through repeated NBNS registrations and outbound activity.

Malware Activity:

Dridex malware confirmed via suspicious domain and HTTP requests such as GET /invest_20.dll

Analysis Screen Shots

Encrypted Traffic View (TCP Stream)

By following the TCP stream, we observe encrypted HTTPS traffic. At this point, the payload contents are unreadable, only encrypted data is visible. This indicates that malicious behavior may be hidden within encrypted channels.

Decrypted Traffic View (TLS Stream)

By following the TLS stream, partial decryption was possible using available session keys. While full payload content remained inaccessible due to incomplete certificate data, the process exposed some previously hidden HTTP requests within the encrypted traffic.

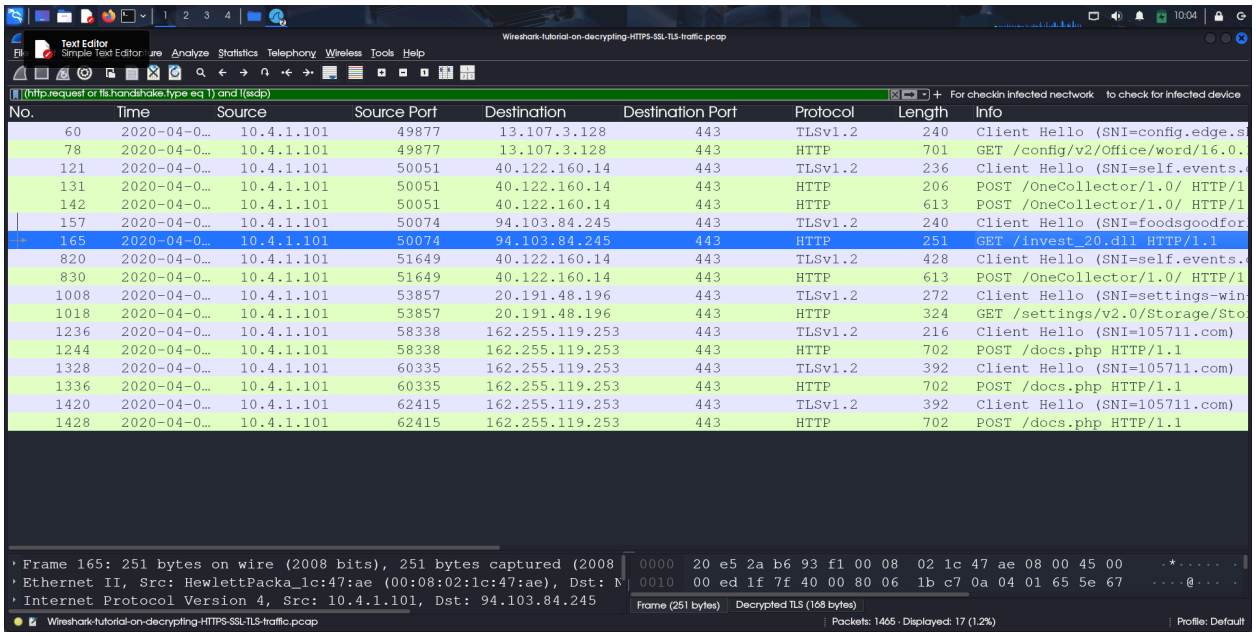
Malicious DLL File (Dridex Variant)

Analysis revealed a malicious DLL file, typical of Dridex variants that inject code into legitimate processes.

After decrypting the HTTPS traffic, HTTP requests to microsoft.com and skype.com were revealed, likely part of routine system processes.

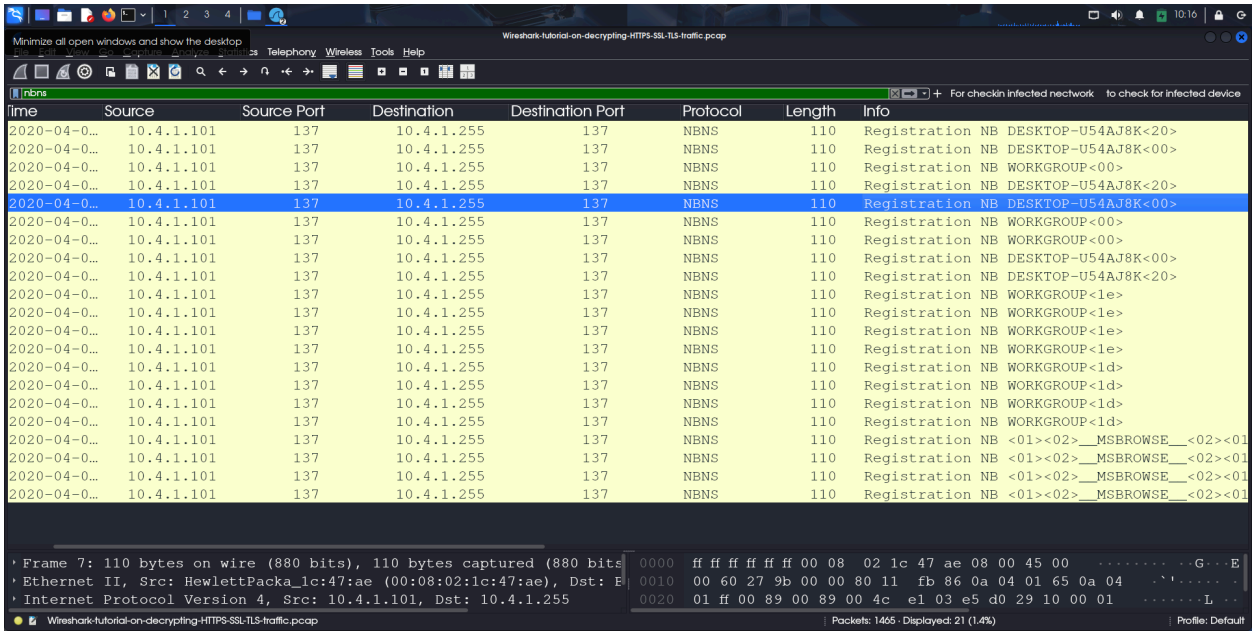
However, the following malicious traffic indicates Dridex malware activity:

- GET /invest_20.dll
  Captured in the screenshot as a direct HTTP request to download a malicious DLL payload used to trigger the infection.



Infected System Identified

The source IP 10.4.1.101 was repeatedly broadcasting NBNS traffic, identifying itself as DESKTOP-U54AJ8K.



Conclusion

Through partial decryption of TLS traffic using available session keys, limited visibility was gained into previously encrypted communications. Although full payload inspection wasn't possible, key indicators of compromise were uncovered. The infected device was observed communicating with suspicious endpoints, leading to the download of a .dll file, a common method for malware delivery. Follow-up POST requests further confirmed malicious activity consistent with Dridex behavior. This underscores the importance of encrypted traffic analysis in identifying infection stages, even when decryption is incomplete.